Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 9. Übung im SoSe 2017:
Praktische IT-Sicherheit

9.1 Aufgaben des IT-Sicherheits-beauftragten

Aufgabe:

- Ein Unternehmen möchte einen **IT-Sicherheitsbeauftragten** einsetzen. Dessen Aufgaben sollen in der Leitlinie zur Informationssicherheit festgeschrieben werden. Dabei sollen insbesondere die Maßnahmen M 2.193, M 2.199, M 2.201, M 2.337 und M 6.58 aus den IT-Grundschutzkatalogen sinnvoll integriert werden (Maßnahmen abrufbar auf https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html). Formulieren Sie den entsprechenden Part zum IT-Sicherheitsbeauftragten für die Leitlinie zur Informationssicherheit!

9.1 Aufgaben des IT-Sicherheits-beauftragten (1)

Aufgaben nach M 2.193 (Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit):

- Steuerung und Koordination des Informationssicherheitsprozesses
  → Prozessverantwortung bei ITSB
- Unterstützung der Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit
  → Verantwortung für Informationssicherheit bleibt bei Leitung
- Koordination der Erstellung von
  ° IT-Sicherheitskonzept
  ° Notfallvorsorgekonzept
  ° und anderer Teilkonzepte und System-Sicherheitsrichtlinien
  → Konzeption der IT-Sicherheit (= Prozessdefinition)
- Erlass weiterer Richtlinien und Regelungen zur Informationssicherheit
  → Genehmigungsinstanz für Richtlinien und Regelungen

9.1 Aufgaben des IT-Sicherheits-beauftragten (2)

Aufgaben nach M 2.193 (Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit): 1. Fortsetzung

- Erstellung des Realisierungsplans für die IT-Sicherheitsmaßnahmen, Initiierung und Prüfung von deren Realisierung
  → Maßnahmenverantwortung (erfordert entsprechendes Budget!)
- Bericht über den Status Quo der Informationssicherheit an Leitungs-ebene und dem Informationssicherheits-Management-Team
  → Rechenschaftsbericht gegenüber Leitungsebene
  → Vorsitz im Informationssicherheits-Management-Team
- Koordination sicherheitsrelevanter Projekte
  → alle Projekte mit Bezug zur IT-Sicherheit bedürfen der aktiven Be-teiligung des ITSB
- Sicherstellen des Informationsflusses zwischen Bereichs-IT, Projekt- sowie IT-System-Sicherheitsbeauftragten

9.1 Aufgaben des IT-Sicherheits-beauftragten (3)

Aufgaben nach M 2.193 (Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit): 2. Fortsetzung

- Untersuchen sicherheitsrelevanter Zwischenfälle
  → Verantwortung für Sicherheitsvorfall-Management
- Initiieren und Steuern von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit
  → Planung von Awareness-Maßnahmen
- Beteiligung bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben
- Beteiligung bei der Einführung neuer Anwendungen und IT-Systeme
- Beteiligung bei der Beschaffung von IT-Systemen
- Beteiligung bei der Gestaltung von IT-gestützten Geschäftsprozessen
- Ausübung der Funktion als Stabsstelle unterhalb der Leitungsebene

9.1 Aufgaben des IT-Sicherheits-beauftragten (4)

Aufgaben nach M 2.199 (Aufrechterhaltung der Informationssicherheit):

- Regelmäßige Überprüfung aller Sicherheitsmaßnahmen (i.d.R. jährlich, teilweise auch unangemeldet)
- Regelmäßige Überprüfung der korrekten Umsetzung als auch der Umsetzbarkeit eines Sicherheitskonzepts mit
  - ° Prüfung von Eignung und Effizienz der Maßnahmen im Hinblick auf die gesteckten IT-Sicherheitsziele (Vollständigkeit & Aktualität)
  - ° Kontrolle der Umsetzung der IT-Sicherheitsmaßnahmen in den einzelnen Bereichen (Revision)
- Umsetzung der im Sicherheitskonzept geplanten Sicherheitsmaßnahmen gemäß dem Realisierungsplan
- Dokumentation des Umsetzungsstandes
- Überwachung und Steuerung der Zieltermine und des Ressourceneinsatzes

9.1 Aufgaben des IT-Sicherheits-beauftragten (5)

Aufgaben nach M 2.199 (Aufrechterhaltung der Informationssicherheit):
1. Fortsetzung

- Anpassung der bestehenden Sicherheitsmaßnahmen aufgrund der Erkenntnisse aus
  - ° sicherheitsrelevanten Zwischenfällen
  - ° Veränderungen im technischen oder technisch-organisatorischen Umfeld
  - ° Änderungen von Sicherheitsanforderungen
  - ° Änderungen von Bedrohungen
- Dokumentation zu den Ergebnissen der einzelnen Überprüfungen
- Einleitung der erforderlichen Korrekturmaßnahmen

9.1 Aufgaben des IT-Sicherheits-beauftragten (6)

Aufgaben nach M 2.199 (Aufrechterhaltung der Informationssicherheit):
2. Fortsetzung

- Unterjährige Prüfungen bei
  - ° Aufbau neuer Geschäftsprozesse, Anwendungen oder IT-Komponenten
  - ° Vornahme größerer Änderungen der Infrastruktur (z.B. Umzug)
  - ° Anstehen größerer organisatorischer Änderungen (z.B. Outsourcing)
  - ° Änderung der Gefährdungslage
  - ° Bekanntwerden gravierender Schwachstellen oder Schadensfälle
- Prüfung der Durchführung aller vorgesehenen Detektionsmaßnahmen (z.B. Auswertung von Protokolldaten)
- Vorschlag einer Korrekturmaßnahme für jede Abweichung
- Information des jeweiligen Vorgesetzten bei Entdecken unzulässiger Aktivitäten von Mitarbeitern

9.1 Aufgaben des IT-Sicherheits-beauftragten (7)

Aufgaben nach M 2.199 (Aufrechterhaltung der Informationssicherheit):
3. Fortsetzung

- Auswertung externer Wissensquellen, wie Standards oder Fachpublikationen
- Kontakte zu Gremien und Interessengruppen, die sich mit Sicherheitsaspekten beschäftigen (Praxisaustausch)
- Dokumentation des Sicherheitsprozesses
- Sicherstellen, dass Auditoren, die Prüfungen vornehmen, nicht an der Konzeption beteiligt waren
- Sicherstellen, dass nur Befugte Zugriff auf Audit- oder Diagnosewerkzeuge und die dokumentierten Prüfungsergebnisse haben

9.1 Aufgaben des IT-Sicherheits-beauftragten (8)

Aufgaben nach M 2.201 (Dokumentation des Sicherheitsprozesses):

- Dokumentation zum Ablauf des IT-Sicherheitsprozesses
- Dokumentation zu wichtigen Entscheidungen im IT-Sicherheitsprozess
- Dokumentation zu den Arbeitsergebnissen der einzelnen Phasen des IT-Sicherheitsprozesses
- Archivierung der Vorgängerversionen der Dokumentationen zum IT-Sicherheitsprozess (→ Nachvollziehbarkeit der Entwicklung)
- Dokumentation der Berichte zum Status der Informationssicherheit an die Leitungsebene
- Beachten, dass die **Leitlinie zur Informationssicherheit** die Sicherheitsziele und Sicherheitsstrategie festlegt und von der obersten Leitungsebene festgelegt und veröffentlicht wurde
- Beschreiben der erforderlichen Sicherheitsmaßnahmen und deren Umsetzung im **Sicherheitskonzept**

9.1 Aufgaben des IT-Sicherheits-beauftragten (9)

Aufgaben nach M 2.201 (Dokumentation des Sicherheitsprozesses):
1. Fortsetzung

- Beachten, dass die bereichs- und systemspezifischen Sicherheitsrichtlinien und die Regelungen für den ordnungsgemäßen und sicheren IT-Einsatz auf der Sicherheitsleitlinie aufbauen
- Dokumentation der Sitzungsprotokolle und Beschlüsse des Informationssicherheits-Management-Teams
- Dokumentation der Ergebnisse von Audits und Überprüfungen (inkl. Prüflisten und Befragungsprotokollen)
- Dokumentation von Sicherheitsvorfällen zur Nachvollziehbarkeit aller damit verbundenen Vorgänge und Entscheidungen (inkl. Protokolle und vorfallsbezogener System-Meldungen)
- Dokumentation zu Installations- und Konfigurationsanleitungen

9.1 Aufgaben des IT-Sicherheits-beauftragten (10)

Aufgaben nach M 2.201 (Dokumentation des Sicherheitsprozesses):
2. Fortsetzung

- Dokumentation der Anleitungen für den Wiederanlauf nach einem Sicherheitsvorfall
- Dokumentation von Test- und Freigabeverfahren (Belegfunktion)
- Dokumentation der Anweisungen für das Verhalten bei Störungen und Sicherheitsvorfällen
- Bereitstellen der geltenden Sicherheitsrichtlinien für Mitarbeiter
- Bereitstellen übersichtlicher Merkblätter für den verantwortungsvollen Umgang mit internen Informationen, für die sichere Nutzung von IT-Systemen und Anwendungen sowie zum Verhalten bei Sicherheits-vorfällen für Mitarbeiter
- Bereitstellen von Handbüchern und Anleitungen für die eingesetzten IT-Systeme und Anwendungen

9.1 Aufgaben des IT-Sicherheits-beauftragten (11)

Aufgaben nach M 2.201 (Dokumentation des Sicherheitsprozesses):
3. Fortsetzung

- Beschreibung und zeitnahe Aktualisierung der Meldewege und der Vorgehensweise für den Informationsfluss zum Sicherheitsprozess

9.1 Aufgaben des IT-Sicherheits-beauftragten (12)

Aufgaben nach M 2.337 (Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse):

- Abstimmen der Methoden zum Risikomanagement aus dem Bereich der Informationssicherheit mit bereits etablierten Methoden der gesamten Einrichtung (→ Einbinden der IT-Risiken in allgemeine Risiken)
- Beitragen zur Widerspruchsfreiheit in Arbeitsanweisungen oder Dienstvereinbarungen aus unterschiedlichen Bereichen
- Beitragen zur klaren Definition von Zuständigkeiten und Kompetenzen unter Berücksichtigung von Vertretungsregeln
- Beitragen zur Planung, Beschreibung, Einrichtung und Bekanntgabe der Kommunikationswege mit Festlegung der Aufgaben, Rollen und des Umfangs der zu kommunizierenden Informationen
- Unterstützt werden durch Fachverantwortliche bei der Erarbeitung und Umsetzung der Sicherheitsstrategie

9.1 Aufgaben des IT-Sicherheits-beauftragten (13)

Aufgaben nach M 2.337 (Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse): Fortsetzung

- Beteiligung an der Einweisung der Mitarbeiter in die erforderlichen Sicherheitsmaßnahmen
- Beteiligung an der Sensibilisierung für Risiken und Schutzvorkehrungen im alltäglichen Umgang mit Informationen
- Überblick über alle Arten von Dienstleistern (sowohl für die Verarbeitung geschäftsrelevanter Informationen als auch für allgemeine Unterstützungsleistungen) und Einschätzung, welche Sicherheitsvorkehrungen diese Dienstleister zu treffen haben

9.1 Aufgaben des IT-Sicherheits-beauftragten (14)

Aufgaben nach M 6.58 (Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen):

- Vorbereitung der Einrichtung auf den angemessenen Umgang mit Sicherheitsvorfällen aller Art
- Etablierung einer geeigneten Vorgehensweise zur Behandlung von Sicherheitsvorfällen
- Klare Definition der Abläufe und Regeln für die verschiedenen Arten von Sicherheitsvorfällen
- Abstimmung mit dem Notfallmanagement
- Entgegennahme von Meldungen über Sicherheitsvorfälle
- Entscheidung über die Einstufung als Sicherheitsproblem oder Sicherheitsvorfall
- Einschaltung des Eskalationswegs bei Sicherheitsvorfällen
- Einleitung notwendiger Maßnahmen zu Sicherheitsvorfällen

9.1 Aufgaben des IT-Sicherheits-beauftragten (15)

Text für Leitlinie zur Informationssicherheit:

Es wird die Funktion eines IT-Sicherheitsbeauftragter eingerichtet, die als Stabstelle der Leitung folgende Aufgaben wahrnimmt:

1. Konzeption der Leitlinie zur Informationssicherheit, die von der Leitung verabschiedet wird
2. Konzeption des Informationssicherheitsprozesses, das von der Leitung verabschiedet wird
3. Regelmäßige Berichterstattung an die Leitung zur aktuellen Sicherheitslage und Vortragsrecht gegenüber der Leitung zu Fragen der Informationssicherheit
4. Information von Fachverantwortlichen über von Beschäftigten verursachte IT-Sicherheitsvorfälle
5. Erlass aller sicherheitsspezifischen Richtlinien und Regelungen im Einklang mit der Leitlinie und dem Sicherheitsprozess

9.1 Aufgaben des IT-Sicherheits-beauftragten (16)

Text für Leitlinie zur Informationssicherheit: 1. Fortsetzung

Es wird die Funktion eines IT-Sicherheitsbeauftragter eingerichtet, die als Stabstelle der Leitung folgende Aufgaben wahrnimmt:

6. Festlegung und regelmäßige Überprüfung der Maßnahmen zur Gewährleistung von Informationssicherheit
7. Abwicklung von IT-Sicherheitsvorfällen
8. Planung von Awarenessmaßnahmen zur Informationssicherheit
9. Einweisung der Beschäftigten zur Informationssicherheit
10. Erstellung von Merkblättern und Anleitungen zur Informationssicherheit
11. Dokumentation aller gültigen Regelungen zur Informationssicherheit und vorgefallener IT-Sicherheitsvorfälle
12. Dokumentation zu durchgeführten Sicherheitsaudits
13. Konsultation zur Informationssicherheit bei allen IT-Projekten

9.1 Aufgaben des IT-Sicherheits-beauftragten (17)

Text für Leitlinie zur Informationssicherheit: 2. Fortsetzung

Es wird die Funktion eines IT-Sicherheitsbeauftragter eingerichtet, die als Stabstelle der Leitung folgende Aufgaben wahrnimmt:

14. Konsultation bei wesentlichen Änderungen beim Ablauf der Geschäftsprozesse und beim Outsourcing, der mit einem Zugriff auf Informationen verbunden ist
15. Konsultation bei der Gestaltung des allgemeinen Risikomanagements zur adäquaten Einbeziehung festgestellter IT-Risiken

9.2 Sicherheitskonzept Telearbeit

Aufgabe:

- Entwerfen Sie ein **Sicherheitskonzept** zur Nutzung von Laptops, mit denen im Zuge von Telearbeit (Home Office oder Außendienst) auch vertrauliche Daten bearbeitet und an den eigentlichen Unternehmens-standort übertragen werden!

9.2 Sicherheitskonzept Telearbeit (1)

- Festplatte des Laptops gemäß dem Stand der Technik verschlüsseln
- systemseitiges Abklemmen externer Laufwerke & Wechseldatenträger; Einrichtung eines Boot-Schutzes
- kein Zugriff auf Betriebssystemebene und Konfigurationen der eingesetzten IT-Komponenten (→ Nutzerrechte, keine Administrationsrechte)
- vorzugsweise Identifizierungs- und Authentisierungsmechanismus mittels Smartcard- oder Fingerabdruckverfahren
- monatliche Änderung der Zugangs- und Zugriffspassworte durch den Beschäftigten unter Einhaltung der Komplexitätsvorschriften
- Erschwerung mehrfach missglückter Neuanmeldeversuche (durch Geringhalten zulässiger Fehlversuche und sukzessive Erhöhung der Zeitabstände für erneute Versuche)
- Automatische Bildschirmsperre bei fehlender Aktivität von 10 Minuten und deren Aufhebung nur mittels Authentifizierung

9.2 Sicherheitskonzept Telearbeit (2)

- Konfiguration minimal entsprechend der zu erfüllenden Aufgaben
- Protokollierung aller sicherheitsrelevanten Aktivitäten
- Virenscanner so installieren, dass dieser bei jeder Anmeldung am LAN und in regelmäßigen Abständen auch während einer bestehenden Verbindung automatisch aktualisiert wird
- kein freier Zugriff auf das Internet
- Freischaltung nur der zur Aufgabenerfüllung zwingend erforderlichen Ports
- Kommunikation zwischen Laptop und LAN nur unter Ausnutzung einer dem Stand der Technik entsprechende starke Transportverschlüsselung (üblicherweise Triple-DES); ein Verbindungsaufbau darf nur nach ausdrücklicher Bestätigung durch den Beschäftigten erfolgen
- Absicherung einer erfolgreichen Datenübertragung mittels Quittierungsverfahren

9.2 Sicherheitskonzept Telearbeit (3)

- zur Telearbeit dürfen ausschließlich gestellte IT-Komponenten (Hardware und Software) eingesetzt, an den Einstellungen keine Änderungen vorgenommen und keine weiteren IT-Komponenten angeschlossen werden
- Zutrittsrecht des Arbeitgebers zum Telearbeitsplatz ist mit dem Beschäftigten zu vereinbaren
- Laptop ist in einem klar separierten und verschließbaren Arbeitszimmer so aufzustellen, dass keine unbefugte Einsichtnahme auf den Bildschirm (weder im Zuge des Betretens des betreffenden Arbeitszimmers noch durch Beobachtung durch etwaige Fenster) stattfinden kann
- streng vertrauliche Unterlagen dürfen außerhalb der Arbeitszeit bzw. Tätigkeit des betreffenden Beschäftigten ausschließlich in verschließbaren Behältnissen gelagert werden

9.3 Serversicherheit

Aufgabe:

- Listen Sie empfehlenswerte Maßnahmen zur **Serversicherheit** auf!

9.3 Serversicherheit (1)

Serversicherheit = Sicherheit der eingesetzten Server

→ Physische Sicherheit der Server + Vorgaben zur Administration von Servern

- Zugangsbefugnis nur für Administratoren
- Nicht mehr benötigte Zugangsberechtigungen unverzüglich entziehen
- Zugangsmittel, wie z.B. Chipkarten, Token, Kennwörter, PIN, etc., vor unbefugter Verwendung sichern
- Vergabe von Zugangsberechtigungen vorzugsweise durch andere Administratoren (soweit möglich) → keine Selbstbefugniserteilung
- Verwendung starker Kennwörter zur Administration:
  ° ausreichende Länge (mind. 12-stellig; für User reicht 8-stellig)
  ° mit aktivierten Komplexitätsregeln
  ° mit ausreichend kurzer Zeitspanne (max. 3 Monate)
- Administrative Passwörter nicht serverseitig im Klartext speichern
- Keine Verwendung allgemeiner Administrationsaccounts (wie z.B. „Admin“ oder „System“) oder voreingestellter Default-User (→ personalisierten Administrationsaccount einsetzen)

9.3 Serversicherheit (2)

- Fernzugriff auf Serversysteme nur über eine nach aktuellem Stand der Technik verschlüsselte Verbindung
- Voreingestellte Standardpasswörter ändern, bevor ein Server produktiv genutzt wird; Änderung vor Produktivsetzung prüfen
- Prüfen, ob Serversysteme bei Eintritt eines Fehlerfalls über sichere und ausreichend robuste Default-Einstellungen verfügen, um einen Wiederanlauf in der vorgesehenen Zeit zu ermöglichen
- Die Überwindung eines einzigen Sicherheitsmechanismusses darf nicht zur Kompromittierung des gesamten Serversystems führen
- Serversysteme dürfen nur solche Fehlermeldungen an Benutzer senden, die nicht unnötig interne Konfigurationszustände offenbaren; dies gilt vor allem im Rahmen des Anmeldeverfahrens an einem Serversystem
- Inaktive Sitzungen nach Ablauf einer kurzen Zeitspanne systemseitig beenden
- Stets alle erforderlichen Sicherheitspatches zeitnah einspielen
- Serversysteme härten (→ Entfernung nicht benötigter Dienste & Ressourcen)

9.3 Serversicherheit (3)

- Bei der Aktualisierung von Software prüfen, ob die vorgenommene Härtung danach weiterhin Bestand hat oder ggf. in der neuen Version entsprechend nachgezogen werden muss
- Für eingesetzte Hardware & Software muss für vorgesehene Einsatzdauer ein ausreichender Support des jeweiligen Herstellers bzw. Distributors bzw. der entwickelnden Stelle zugesichert sein
- Gespeicherte Daten müssen für Dauer der Aufbewahrungsfrist weiterhin lesbar sein (→ ggf. rechtzeitig in migrationsfähigem Format auf anderes Serversystem umziehen)
- Regelmäßiger Sicherheitscheck der eingesetzten Serversysteme
- Verfolgung abrufbarer Schwachstellenmeldungen zu den eingesetzten Serversystemen
- Wenn ein Server einem Angriff ausgesetzt ist, sollte dies einen aufgezeichneten Event auslösen, der zeitnah vom zuständigen Administrator bearbeitet werden kann

9.4 Sicherheitsprobleme VoIP

Aufgabe:

- Welche sicherheitsbezogenen Probleme sind Ihrer Ansicht nach bei der Einrichtung von **Voice over IP** zu adressieren?

9.4 Sicherheitsprobleme VoIP

- Schutz vor einer Kompromittierung der Unverletzlichkeit des Wortes und Mitschnitt von Kommunikationsverbindungen gewährleisten, da Sprachdaten über IP übertragen und auf Server gespeichert werden
  → Verschlüsselung ohne Performanceverlust!
- Gewährleistung der Zugriffs-/Weitergabekontrolle nach Datenschutz
- Maßnahmen gegen versuchte Verhinderung des Zustandekommens der Kommunikation (z.B. durch Vortäuschen des Besetzzeichens)
- Verhinderung von Abrechnungsbetrug (z.B. mittels Konfiguration eines 0190-Rufzugangs durch Angreifer)
- Umgang mit den (funktionsbedingten) Schwachstellen des IP:
  - Vortäuschen einer falschen Identität
  - Fälschung von Übermittlungsadressen
  - Fälschung von Registrierungsinformationen

  → Man-in-the-Middle-Attack bzw. Call-Hijacking
- Maßnahmen gegen DoS-Attacken mittels SYN-Flooding
- Umgang mit SPAM over Internet Telephony (SPIT)

9.5 Interessenausgleich zwischen Betroffene & Systemnutzer

Aufgabe:

- Nennen Sie Beispiele, in denen sich die **Interessen** der **Betroffenen** von den Interessen der **Systemnutzer** deutlich unterscheiden! Welcher Ausgleich wäre in diesen Beispielen ein möglicher Kompromiss?

9.5 Interessenausgleich zwischen Betroffene & Systemnutzer

Beispiele für abweichende Interessen:

- Systemnutzer möchten möglichst detaillierte Daten angezeigt bekommen, um sicher gehen zu können, dass sie keine fehlerhaften Daten eingeben bzw. bearbeiten. Betroffene möchten, dass verantwortliche Stellen nur so viel Daten über sich haben, wie unbedingt nötig. Der Ausgleich erfolgt daher durch das **Berechtigungskonzept**, in dem festgelegt ist, welcher Nutzer welche Daten (zu welchem Zweck) einsehen und bearbeiten darf.
- Systemnutzer wünschen eine umfassende Datensicherung, damit im Falle eines ungewollten Datenverlustes oder bei einem zeitlich späteren Vorgang noch die Historie berücksichtigt werden kann. Betroffene möchten, dass ihre Daten nur für die vorgeschriebene Dauer abrufbar sind. Der Ausgleich erfolgt daher über die Regelungen zur **Sperrung** (= „Einschränkung“ nach EU-DSGVO) von Daten.